DAVID H. HARPER (*Pro Hac Vice*)
david.harper@haynesboone.com
JASON P. BLOOM (*Pro Hac Vice*)
jason.bloom@haynesboone.com
HAYNES AND BOONE, LLP
2801 N Harwood St., Suite 2300
Dallas, Texas 75201
Telephone: (214) 651-5000
Facsimile: (214) 651-5940

JASON T. LAO, SBN 288161
jason.lao@haynesboone.com
ANDREA LEVENSON, SBN 323926
andrea.levenson@haynesboone.com
HAYNES AND BOONE, LLP
600 Anton Boulevard, Suite 700
Costa Mesa, California 92626
Telephone: (949) 202-3000
Facsimile: (949) 202-3001

Attorneys for Plaintiff
X Corp.

Colin R. Kass (*pro hac vice*)
PROSKAUER ROSE LLP
1001 Pennsylvania Ave., N.W.
Washington, D.C. 20004
(202) 416-6890
ckass@proskauer.com

David A. Munkittrick *(pro hac vice)*
PROSKAUER ROSE LLP
Eleven Times Square
New York, New York 10036
(212) 969-3000
dmunkittrick@proskauer.com

Attorneys for Bright Data Ltd.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

X CORP., a Nevada corporation,

Plaintiff,

vs.

BRIGHT DATA LTD., an Israeli corporation,

Defendant.

Case No. 3:23-cv-03698-WHA

JOINT NOTICE REGARDING PROPOSED PROTECTIVE ORDERS

Hon. William Alsup

Plaintiff X Corp. and Defendant Bright Data Ltd. have agreed on almost all of the provisions of a Proposed Protective Order governing confidential information. The parties met and conferred in good faith and reached agreement on all but one issue: whether two designated in-house counsel should have access to information designated as "Highly Confidential." The parties respectfully request the Court's assistance in resolving this issue. The parties have agreed to submit this Joint Notice to explain their respective positions, with each party agreeing to limit its argument to five pages or less. The parties are prepared to address the issues promptly via telephone conference or hearing at the Court's discretion.[1]

[1] Attached as **Exhibit A** is X Corp.'s Proposed Protective Order, and attached as **Exhibit B** is Bright Data's Proposed Protective Order. For the Court's convenience, attached as **Exhibit C** is a Table of Disputed Provisions. Attached as **Exhibit D** is a declaration from Bright Data's Chief Technology Officer Ron Kol in support of Bright Data's position. Attached as **Exhibit E** is the Model Protective Order for the District of New Jersey submitted by Bright Data.

I. X CORP.'S STATEMENT

X Corp.'s proposed Protective Order tracks this Court's "Model Protective Order for Litigation Involving Patents, Highly Sensitive Confidential Information and/or Trade Secrets," including the Model Protective Order's option to allow up to two designated in-house counsel not involved in competitive decision-making to view documents labeled as "Highly Confidential."[2] Bright Data disputes the inclusion of this provision and would, instead, block designated in-house counsel from viewing "Highly Confidential" documents.

Blocking two specifically designated in-house counsel from accessing Highly Confidential materials would significantly impair X Corp.'s ability to investigate its claims and defenses and outside counsel's ability to communicate with X Corp.'s in-house counsel about what it anticipates will be the majority of Bright Data's documents and deposition testimony, as well as related litigation strategy. If X Corp.'s two designated in-house counsel are not permitted to see "Highly Confidential" documents, Bright Data will be incentivized to designate the majority of its documents as "Highly Confidential" in order to keep X Corp. in the dark. In fact, Bright Data initially proposed having ***all*** documents automatically designated as "Highly Confidential," demonstrating that the risk of over-designation is real. Additionally, the Model Protective Order is tailored to mitigate the risk of disclosure of confidential information to unauthorized parties. *See Barnes & Noble, Inc. v. LSI Corp*., No. C 11-02709 EMC LB, 2012 WL 601806, at *1 (N.D. Cal. Feb. 23, 2012) ("the court treats the model protective order as setting forth presumptively reasonable conditions regarding the treatment of highly confidential information"). In short, X Corp.'s proposed Protective Order, attached hereto as **Exhibit A**, should be entered by the Court.

Denying designated in-house counsel the opportunity to review Highly Confidential information would significantly impair X Corp.'s ability to prosecute its claims by preventing outside counsel from discussing what X Corp. anticipates will be the majority of Bright Data's document production with designated in-house counsel. Bright Data has indicated its intention to broadly use the "Highly Confidential" designation in a few ways. First, Bright Data initially

[2] X Corp. revised the Model Protective Order to omit certain footnotes and other provisions that are not relevant to this dispute, and the parties do not dispute these revisions.

proposed a protective order that would have ***automatically*** designated ***all*** documents, discovery responses, and depositions as "Highly Confidential." While Bright Data has backed off that proposal, it illustrates Bright Data's intent to broadly designate its documents and deposition testimony as "Highly Confidential" and thereby prevent designated in-house counsel from viewing it. In another scraping case involving Bright Data in this District (albeit involving different Terms of Service), Bright Data has shown its propensity to over-designate discovery to impede the litigation. *See Meta Platforms, Inc. v. Bright Data Ltd*., No. 23-CV-00077-EMC (N.D. Cal. Jan. 6, 2023) (Dkt. 188). In that case, Bright Data refused to permit Meta's in-house counsel to attend any of the jurisdictional discovery depositions of Bright Data and then designated all of those depositions as Highly Confidential, based on the purported "substantial commercial harm" that could result. Bright Data sought to seal those depositions in their entirety, while at the same time relying on them in motion practice. *Id.* Bright Data's proposed Protective Order attempts to repeat that playbook in this case.

X Corp. therefore has serious concerns that Bright Data will attempt to use the "Highly Confidential" designation to shield virtually ***all*** documents and depositions from view of designated in-house counsel. X Corp.'s claims require the assistance of in-house counsel to review—and dispute—the assertions made by Bright Data regarding its scraping activity on the X platform. This knowledge is crucial to X Corp.'s ability to effectively prosecute this case.

The Model Protective Order submitted by X Corp. sufficiently addresses any concerns Bright Data may have about two designated in-house counsel seeing its "Highly Confidential" information *See Barnes & Noble*, 2012 WL 601806, at *1. In considering the extent of in-house counsel's access to confidential information, courts must balance (1) the risk of inadvertent disclosure of a party's confidential information against (2) the risk that protection of the confidential information would impair the other party's prosecution of its claims. *Brown Bag Software v. Symantec Corp*., 960 F.2d 1465, 1470 (9th Cir.1992). First, under X Corp.'s proposed Protective Order, before "Highly Confidential" information may be shown to designated in-house counsel, the proposed designated counsel and their job duties must be disclosed to opposing

counsel.[3] Second, designated in-house counsel may not be involved in competitive decision-making and must agree to be bound by the Protective Order.[4] Third, opposing counsel may object to having Highly Confidential information disclosed to designated in-house counsel and present the issue to the court if not resolved between the parties.[5] Fourth, designated in-house counsel are not permitted to review source code.[6] *See Barnes & Noble*, 2012 WL 601806, at *2 (identifying competitive decision-making as the "crucial factor" in determining the risk of disclosure).

In light of the above, Bright Data's concerns are baseless. Bright Data and X Corp. are not competitors. Further, by opposing the disclosure of "Highly Confidential" information to two designated in-house counsel under the Model Protective Order's provisions, Bright Data is asserting, without any evidence, that X Corp.'s designated in-house counsel—who would necessarily be lawyers with no involvement in competitive decision making regarding X Corp.'s technological defenses to Bright Data's scraping—intend to violate their own ethical duties and the Court's Protective Order, which they will be required to acknowledge in a signed writing. That Bright Data would make such a baseless and unsupported assertion underscores Bright Data's true objective, which is to hobble X Corp.'s ability to effectively prosecute its claims by restricting access to discovery.

In short, X Corp.'s proposed protective order tracks the Court's model order and provides sufficient safeguards to prevent harm to Bright Data. X Corp. respectfully asks this Court to enter the Protective Order proposed by X Corp.

[3] *See* Ex. A at § 7.4(a)(1).

[4] *See* Ex. A at § 7.3(b).

[5] *See* Ex. A at § 7.4(b), (c).

[6] X Corp.'s proposed § 7.3(b) states that the procedures in § 7.4(a)(1) must be complied with before Designated House Counsel can see Highly Confidential information, and § 7.4(a)(1) does not provide for the disclosure of Source Code. Further, the final clause of § 8(b) in X Corp.'s proposed Protective Order—which Bright Data deleted—specifically confirms that Designated House Counsel may not see Source Code.

II. BRIGHT DATA'S STATEMENT

Protective orders facilitate the exchange of information while minimizing the risk of collateral injury from disclosure of sensitive information. The Model Protective Order strikes the right balance by presumptively limiting access to Highly Confidential Information to outside counsel. X seeks to reverse this presumption, giving in-house counsel carte blanche to review virtually *everything* Bright Data produces. But there is no reason to depart from the Model here. X does not explain why in-house counsel needs access to *any* Highly Confidential Information. Nor does it make a tailored, information-specific showing of need. Its proposal should be rejected.

X seeks to impose an "optional" provision that was designed for different circumstances. The option allows, upon agreement of the parties, in-house counsel access to some (but not all) Highly Confidential Information "as … appropriate in case-specific circumstances."[7] The option works for cases where the parties have no incentive or ability to misuse the information. In such cases, the Highly Confidential designation mainly protects against third-party disclosure. For example, in a simple vendor-vendee contract dispute, the parties may not compete, so there would be no information deemed "competitively sensitive" vis-à-vis each other. That same information, of course, may still be highly sensitive as to other third parties, in which case the optional provision may work there. But that is not this case.

This case epitomizes why the in-house counsel option should not be imposed over Bright Data's objection. X is trying to shut Bright Data down.[8] It is one thing to do so through a legal ruling; it is quite another to do so by gaining access to Bright Data's most sensitive information

[7] Even where the parties agree to this "optional" provision, the Model notes that the parties should consider limiting in-house counsel's access to information "only if it is filed with the court under seal, or in the presence of Outside Counsel of Record at their offices." Model Order at n.4, *available at* https://www.cand.uscourts.gov/wp-content/uploads/forms/model-protective-orders/ND_Cal_Patent_Highly_Sensitive_Model_Prot_Ord_Revised.docx. X's proposal does not have any of these limitations.

[8] It is well documented that X is engaged in a "crusade" against web scrapers, and is ***improperly*** using litigation as a means of advancing its cause. *See* https://www.calcalistech.com/ctechnews/article/b11s3ovc3 ("Elon Musk's ***crusade*** [against Bright Data and other web scrapers] isn't about protecting data privacy, but leveraging data for himself"). Last year, X filed a lawsuit against "John Doe" scrapers in Texas. *See X Corp. v. John Does 1-11*, No. DC-23-09157 (Dallas Cty July 19, 2023). A suit against only "Does," obviously cannot be served, and is only an improper attempt to use litigation to issue subpoenas. In that case, the effort failed, and costs were awarded against X. *Id*. Here, while X has targeted a real defendant, that is no license to use the discovery process for such ancillary purposes.

with which X could take ***marketplace actions*** to achieve victory through business conduct regardless of its legal case. Here, X has requested some of Bright Data's most sensitive information. Under the Model Protective Order, the producing party must make a document-by-document confidentiality determination and can only designate information as Highly Confidential if it is likely to cause significant competitive harm. As Bright Data's Chief Technology and Security Officer explains, Bright Data will suffer significant harm if this information is disclosed to X. *See* Ex. D. In brief, these harms include:

- Using Bright Data's search-identifiable information, such as IP addresses, server information, and crawl scripts to technologically block lawful scraping by Bright Data and its customers.
- Using Bright Data's engineering documents, source code, and technology specifications to enhance X's own blocking technologies, thereby, reducing or interfering with the reliability of Bright Data's own services.
- Using Bright Data's customer-identifiable information to terminate accounts of overlapping customers, restrict their access to information, target them for future enforcement actions, or otherwise encourage them to cease lawful scraping.

Giving access to X's in-house counsel is particularly problematic because they are on the front lines of taking action to stop scraping of X's site. It would be giving the fox free access to the hen house. The Model's in-house "option" was never intended to do that.

X does not present any "case-specific circumstances" that warrant disclosure of Highly Confidential Information to in-house counsel. Its only argument to depart from the Model is ***baseless*** speculation that Bright Data will over-designate. X is not entitled to assume that Bright Data will violate this Court's order by improperly designating materials. And, if there is over-designation, the Protective Order has specific procedures to address it.[9]

[9] Indeed, the two facts X presents to support its speculation undermines. *First*, it complains that Bright Data proposed (during the meet and confer) a process that would allow for presumptive designation of materials. But Bright Data is not asking the Court to include these provisions, even though other courts in this District have done so over a party's objection. *Mathew Enter., Inc. v. Chrysler Group LLC*, 2015 U.S. Dist. Lexis 1657 (N.D. Cal. 2015). X's argument, that Bright Data will disregard its obligations under the Order just because it proposed something different, is frivolous. Second, X complains that Meta has opposed Bright Data's sealing motion in a different case. As an initial matter, Bright Data did not seek to seal a single word of its brief in that case. The only issue there was deposition transcripts, and the period for making line-by-line designations had not yet run under the applicable protective order. The parties here have agreed on the same procedures that govern deposition designations.

Nor does X claim that its in-house counsel has any particularized need for this information. As to Bright Data's technical information, X does not say what in-house counsel would do with it, or even that they have the technical expertise to use it. Indeed, that is one reason for independent experts. Nor does in-house counsel have any need for customer-specific information. What could they possibly do with it? They could send cease-and-desist letters, disable accounts, or share the information with X's engineers, tech specialists, their External Misuse Teams, or other business people to have them "investigate." But each of these would be a violation of the Protective Order. Virtually any use by in-house counsel of this information – other than to simply satisfy their curiosity – would be impermissible. There is no need for them to access Bright Data's Highly Confidential Information in the first place, and certainly not presumptively.[10]

Nor does X argue that its outside counsel is somehow incapable of litigating this case without in-house access to Bright Data's secrets. As one court explained:

> "[The plaintiff] must assess the merits of the litigation and develop strategy using litigation counsel and outside experts to review information marked confidential or attorney eyes only, and present it in a non-confidential manner to the client for decision-making purposes. This is a necessary consequence of achieving a balance between full disclosure in discovery and protection against economic injury."

See McAirlaids, Inc. v. Kimberly-Clark Corp., 299 F.R.D. 498, 501 (W.D. Va. 2014). Restricting in-house counsel's access to Highly Confidential Information will not impede their ability to provide strategic direction. They will have access to Confidential Information, and can challenge any Highly Confidential designation when needed. Nothing prevents outside counsel from discussing the case with in-house counsel, or referring generally to what discovery has shown. Indeed, many courts' model protective orders make this explicit, noting that "[i]t is ... understood that counsel for a party may give advice and opinions to his or her client … based on his or her evaluation of Confidential material, provided that such advice and opinions shall not reveal the

[10] Many courts limit in-house counsel's access to Highly Confidential Information. *See, e.g.*, *Brown Bag Software v. Symantec Corp.*, 960 F.2d 1465, 1471 (9th Cir. 1992); *Ubiquiti Networks, Inc. v. Kozumi USA Corp.*, 2012 U.S. Dist. LEXIS 168351, *4 (N.D. Cal. 2012); *Monster Cable Prods. v. Di Ve Rsified Repackaging Corp.*, 2011 U.S. Dist. LEXIS 90263, *5 (N.D. Cal. 2011); *Shared Memory Graphics, LLC v. Apple, Inc.*, 2010 WL 4704420, *2 (N.D. Cal. 2010); *Acer Am. Corp. v. Tech. Props.*, 2009 WL 1363551, *4 (N.D. Cal. 2009); *Intel Corp. v. VIA Techs., Inc.*, 198 F.R.D. 525, 528 (N.D. Cal. 2000).

content of such Confidential material." Ex. E ¶ 3.

Nor does it matter whether the particular (currently, unidentified) in-house counsel that X would designate may not be involved in "competitive decision-making." Bright Data and X may not directly compete for social media customers, but they joust vigorously every day in the passageways of the Internet, one constantly striving to access public information, and the other constantly striving to block it. Whether or not X's counsel is involved in "competitive decision-making," they can nonetheless destroy Bright Data's business if they get access to Bright Data's underlying technology, IP addresses, search-identifiable information, or customer-identifiable information. *See THX, Ltd. v. Apple, Inc*., 2016 WL 2899506, *2 (N.D. Cal. 2016) ("even if … not a direct competitor …, disclosure could still cause competitive risk"). Nor is the general prohibition against using the information for commercial purposes sufficient. If it were, all protective orders would be limited to a single sentence.

X cannot justify access by the fact that in-house counsel has ethical obligations. Once X's in-house counsel "learns of the confidential information," "it would be manifestly impossible for [them] to perform the mental gymnastics of putting the information out of [their] consciousness" when making decisions regarding X's anti-scraping crusade. *Autotech Techs. Ltd. P'ship v. Automationdirect.com, Inc*., 237 F.R.D. 405, 410-11 (N.D. Ill. 2006). They could no more "do that than the boy in Mark Twain's story who was told to stand in a corner and not think of a white elephant." *Id*.; *Tailored Lighting, Inc. v. Osram Sylvania Prods., Inc.*, 236 F.R.D. 146, 147, 149 (W.D.N.Y. 2006) ("It seems unreasonable to expect that anyone working to further his own scientific and technological interests would be able assuredly to avoid even the subconscious use of confidential information"); *In re Deutsche Bank Tr. Co. Americas*, 605 F.3d 1373, 1378 (Fed. Cir. 2010) (same). X does not deny that in-house counsel are tasked with taking action – both judicially and extra-judicially – against Bright Data and its customers. They are not entitled to Bright Data's Highly Confidential Information just because X filed a Complaint.

To the extent there is a legitimate need for in-house counsel's access to Bright Data's Highly Confidential Information, X can raise it as to particular documents. That is a far better than allowing what is effectively carte blanche access to everything Bright Data will produce.

Dated: February 21, 2024

Respectfully submitted,

HAYNES AND BOONE, LLP

By: /s/*Jason T. Lao*
David H. Harper (*Pro Hac Vice)*
david.harper@haynesboone.com
Jason P. Bloom (*Pro Hac Vice*)
jason.bloom@haynesboone.com
2801 N. Harwood St., Suite 2300
Dallas, Texas 75201
Telephone: (214) 651.5000

Jason T. Lao
jason.lao@haynesboone.com
Andrea Levenson
andrea.levenson@haynesboone.com
600 Anton Boulevard, Suite 700
Costa Mesa, California 92626
Telephone: (949) 202-3000

Attorneys for Plaintiff X Corp.

PROSKAUER ROSE LLP

By: /s/ *Colin R. Kass*
Colin R. Kass (*pro hac vice*)
Proskauer Rose LLP
1001 Pennsylvania Ave., N.W.
Washington, D.C. 20004
(202) 416-6890
ckass@proskauer.com

David A. Munkittrick *(pro hac vice)*
Proskauer Rose LLP
Eleven Times Square
New York, New York 10036
(212) 969-3000
dmunkittrick@proskauer.com

Attorneys for Defendant Bright Data Ltd.

CERTIFICATION

I, Jason T. Lao, am the ECF User whose identification and password are being used to file this JOINT NOTICE REGARDING PROPOSED PROTECTIVE ORDERS. In compliance with Civil L.R. 5-1(h)(3), I hereby attest that each other signatory has concurred in this filing.

Date: February 21, 2024

/s/Jason T. Lao
Jason T. Lao

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this day, a true and correct copy of the foregoing document was served by filing the same via the Court's CM/ECF system, which will provide notice of the filing of same to all counsel of record.

Date: February 21, 2024

/s/Jason T. Lao
Jason T. Lao